

## MEMORANDUM FOR All New England District Employees

## SUBJECT: Policy on Use of Computer Equipment

1. The enclosed memorandum outlines the policy applicable to use of computer equipment throughout CENAE. All supervisors and employees must comply with guidance. This guidance applies to all CENAE local and remote offices.
2. **General:** Many unclassified Army systems allow users to access the Internet. While the Army promotes the use of the Internet to achieve Army goals, appropriate safeguards must be established to prevent and detect technical attacks made on Army systems and to ensure classified or sensitive information is not inadvertently released to unauthorized personnel. Use of the CENAE computer system, including all related equipment, networks and network devices may be monitored for all lawful purposes, including to ensure their use is authorized for management of the system, to facilitate protection against unauthorized access, and to verify security procedures and operational security.
3. **Authorized use:** The Joint Ethics Regulations allow users to make limited use of DOD telephones, e-mail systems, and Internet connections for personal use, so long as such uses are on a not-to-interfere basis and are not for an improper purpose (such as conducting a private business or reviewing pornography). Users will employ Internet access for authorized, unclassified U.S. Government business. Chat sites are not authorized. Users are not to use their private accounts for Army-related business unless specifically authorized to do so by the Director of Information Management (IM). Users are authorized to download and upload programs, graphics, and textual information between the Internet and an unclassified government-owned personal computer. Personnel will scan all files for viruses before storing, transmitting, or processing information within Army computers, systems, or networks. Virus detection software will be installed on every PC and should not be removed by individuals. Further Internet guidelines are provided at Appendix A.
4. **E-Mail:**
  - a. District-wide, e-mail systems are intended for official and authorized use only. Officially sanctioned groups such as union, welfare council, and other "in-house" organizations can be authorized users. E-mail system(s) users will demonstrate common sense, good judgement, and propriety when using district assets.
  - b. District e-mail systems will not be used to transfer:
    - (1) Classified or other proprietary or privileged information, e.g., privacy, contractual, or financial data which requires additional safeguards;
    - (2) Personal messages that could otherwise be conveyed by telephone;
    - (3) Personal messages, which clearly are for self-promotion or personal gain, e.g., advertising articles for sale;

CENAE-DE

SUBJECT: Policy on Use of Computer Equipment

c. District e-mail systems users should keep in mind at all times that:

(1) All message traffic is official in nature, is the property of the government, and is always subject to being monitored by proper authority;

(2) All message traffic must be safeguarded from disclosure to those who have no official requirement to view it;

(3) E-Mail exists to facilitate the staffing process by allowing for the transfer of routine information when the telephone is not appropriate;

(4) District-wide broadcast messages must be held to a minimum and only be released with the cognizant approval of the respective management authority. The District Intranet is the proper media for most messages of general Internet.

4. **Software:** Individuals will not load personally owned or unauthorized commercial software on government computers. The Director of IM will determine whether commercial software is authorized for installation on a government computer. Computer games will not be operated on a government computer. Individuals will not take or copy government owned software for personal usage.

5. **Reporting suspicious activity:** Army Internet sites are considered as lucrative intelligence sources and are targeted for information collection efforts. As stated in AR 380-12, Army personnel must report suspicious activity through Counterintelligence (SAEDA) and OPSEC channels. All suspicious activity should be reported to the CENAE, Information Systems Security Officer, Ms. Sue Robichaud immediately.

Encl

MICHAEL W. PRATT  
COL, EN  
Commanding

## **APPENDIX A**

### **INTERNET USER SECURITY GUIDELINES**

**1. SCOPE:** These guidelines cover any Army-sponsored use of the Internet computer network. These are minimum guidelines for such use and do not exempt users from further restrictions that may be imposed by their MACOMS. A signature on this document signifies awareness of and compliance with governing security policies. These guidelines do not apply to personal e-mail accounts or subscriptions to computer services that an Army employee uses for non-Army related purposes. Users are not to use their private accounts for any Army related business unless specifically authorized by the MACOMS. If such authorization is granted, these guidelines apply to the conduct of Army-related business on personal accounts.

**2. USER RESPONSIBILITIES:** Individuals using their personal or Army-sponsored accounts should use the same kind of discretion in their “electronic on-line relationships” that they would in any private telephone conversation or face-to-face meeting. Misuse of Army-sponsored accounts (chain mail, access for personal gain, etc.) is considered fraud, waste, and abuse, and may be chargeable under UCMJ, OPM regulation, or relevant U.S. Codes.

**3. APPROPRIATE USES OF THE INTERNET:** Army-sponsored accounts may be used for official unclassified U.S. Government business only. Users may not use their U.S. Government access to the Internet for personal purposes. Access to the Internet through Army accounts is subject to monitoring. Consequently, only Army-related business that may be publicly attributed to the Army may be conducted on Army-sponsored accounts. In addition to normal duties, appropriate uses of Army-sponsored accounts include (but is not limited to) the following:

- a. Keeping up with the professional literature of field;
- b. Acquiring publicly available information of value to the Army;
- c. Conducting unclassified contract/COTR-related contact; and
- d. Keeping current with unclassified office matters while on temporary duty.

**4. CONTACTS WITH THE MEDIA AND CONGRESS:** All official contacts with the media concerning Army matters must be made through an appropriate level Army Public Affairs Office and all official contacts with Congress concerning Army matters must be made through the Office of Congressional Liaison.

**5. CONTRIBUTING TO THE INTERNET:** Although Army-sponsored account users may participate in e-mail correspondence and contribute to its publicly accessible services, they may not release official Army information. Only HQDA may authorize the release of information identified as the Army’s official position. In contributing to discussions on publicly accessed Internet services and in e-mail correspondence, users must provide a disclaimer that their views do not represent an official Army position. Even so, users should exercise caution in their posting and correspondence because they and their comments may be identifiable with the Army, the communications may be widely distributed, and hostile intelligence services may be tracking Internet messages originating from Army-sponsored accounts.

**6. LEGAL RESTRICTIONS ON INTERNET USE (Copyright, Title 17, U.S.C.):** Users shall respect the legal protection provided by copyright, license, and authorship of messages, programs, and data on the network. The copyright laws of the United States provide that the owner of copyright (usually the originator of the work) has exclusive rights to reproduce, distribute, prepare derivative works, and publicly display or perform a work. Unless there is specific notice to the contrary, material on the Internet is protected by copyright even if it does not have a copyright notice (such as the “c” in a circle or the word “copyright” followed by a name and date). There is, however, an exception to the copyright statutes-known as the “fair use” exception. Under this exception, it is fair to use a copyrighted work without the owner’s consent where such use is necessary or desirable for the public benefit or welfare and does not exceed reasonable limits. Determinations as to whether a use is “fair” are made on a case-by-case basis by examining such factors as the purpose of the use, the nature of the work, the amount and substantiality of the portion used, and the effect of the use on the value of/or market for the copyrighted work. Users should consult with the Office of General Counsel regarding certain limited exceptions to the Copyright Act’s prohibitions and for additional guidance on this subject.

**7. PRIVACY ACT (5 U.S.C. PARA 552a):** The Privacy Act, like the copyright laws, applies equally to electronic data. The Privacy Act is one of the laws governing the Army’s collection and dissemination of information about U.S. citizens and permanent resident aliens. If such information can be retrieved from an Army records system by the name of the individual or by some other identifying particular (such as a social security number), it is a Privacy Act record. Because of the Privacy Act restrictions, users may not post or send in any manner Privacy Act records outside Army control without guidance from the Office of General Counsel.

**8. PROVISION GOVERNING THE COLLECTION, RETENTION, AND DISSEMINATION OF INFORMATION; CONTACTS WITH THE U.S. PERSONS; AND PARTICIPATION IN ORGANIZATIONS IN THE UNITED STATES (Executive Order 12333):** The E.O. governs Army’s interactions with U.S. persons and our collection, retention, and dissemination of information concerning U.S. persons. Users may not solicit or gather information on the domestic activities of U.S. persons through participation on the Internet. Users should consult with the Office of General Counsel if they have specific concerns regarding U.S. person matters.

**9. INTERCEPTION OF COMMUNICATIONS (Fourth Amendment, Electronic Communications Privacy Act, and Executive Order 12333):** In the U.S., users may not intercept the private transmissions of other users or attempt to access stored electronic communications of others without authorization. Users may, however, access electronic bulletin boards, list servers, and discussion groups that are generally accessible to any member of the public.

**10. RECORD KEEPING:** Internet communications may be considered Federal records. Those that qualify as Army record must be managed according to their information content; therefore, users must follow Army Regulation 25-11 with respect to such records.

**11. UNAUTHORIZED USE:** Any users who fails to follow the Army’s Internet Policy, these guidelines, or any laws or regulations applicable to Internet use is subject to such action as may legally be taken under the CUMJ, OPM regulation, or relevant U.S. Code.